

UNITED STATES DISTRICT COURT

for the  
District of Oregon

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Alan Williams and  
all personal belongings within immediate vicinity and  
control, as described in Attachments A-1 and A-2

Case No. 3:22-mc-01146 - A

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Alan Williams and all personal belongings within immediate vicinity and control, as described in Attachments A-1 and A-2.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachments B-1 and B-2 hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
15 U.S. C. § 78j(b) & 78ff, 17 C.F.R & 240.10b-5	Insider trading securities fraud
18 U.S.C. § 1341	Wire Fraud

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Flynn McFadden

Applicant's signature

Special Agent Flynn McFadden, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone \_\_\_\_\_ (specify reliable electronic means).

Date: December 13, 2022

City and state: Portland, Oregon

Judge's signature

Hon. Jeffrey Armistead, Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT  
DISTRICT OF OREGON

In the Matter of the Application of the United States of America for Search and Seizure Warrants for (1) the Premises Known and Described as 1095 SW Schaeffer Road, West Linn, OR 97068; (2) Any Electronic Devices in the Possession, Custody, or Control of Alan Williams;

USAO Reference No. 2022R0020

**TO BE FILED UNDER SEAL**

**Agent Affidavit in Support of  
Application for Search and Seizure  
Warrant**

DISTRICT OF OREGON) ss.:

Flynn McFadden, Special Agent, Federal Bureau of Investigation, being duly sworn,  
deposes and states:

**I. Introduction**

**A. Affiant**

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI” or “Investigating Agency”) and have been so employed since approximately September 2020. As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am currently assigned to an FBI squad that investigates white collar crimes, including insider trading. During the course of my duties, I have received training about and participated in the execution of search warrants, and the review and analysis of both physical and electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises (the “Subject Premises”) and person (the “Subject Person”) described below for, and to seize, the items and information described in Attachments B-1 and B-2, respectively. This affidavit is based upon my personal

knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

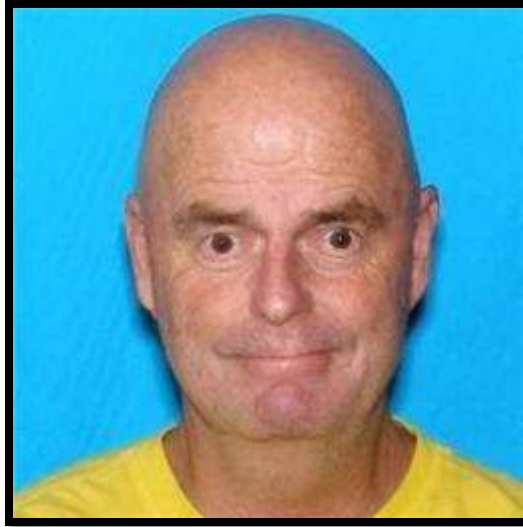
**B. The Subject Premises**

3. The Subject Premises is particularly described as the premises at 1095 SW Schaeffer Road, West Linn, OR 97068. Publicly available photographs of the Subject Premises are shown below:



**C. The Subject Person**

4. The Subject Person to be searched is Alan Williams, who was born on September 3, 1945, (shown in the photograph below), and any and all clothing and personal belongings, backpacks, briefcases, purses, and bags that are within Williams’s immediate vicinity and control at the location where the warrant is executed:



#### **D. The Subject Offenses**

5. For the reasons detailed below, there is probable cause to believe that any electronic devices in the possession of the Subject Person, or found within the Subject Premise, and certain additional materials found within the Subject Premises, as defined below, contain evidence, fruits, and instrumentalities of violations of 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b-5 (insider trading securities fraud); 18 U.S.C. § 1343 (wire fraud); and aiding and abetting and conspiring to commit these offenses in violation of 18 U.S.C. §§ 2 (aiding and abetting), 371 (conspiracy), and 1349 (conspiracy) (the “Subject Offenses”).

## **II. Probable Cause**

### **A. Probable Cause Regarding Subjects’ Commission of the Subject Offenses**

6. Based on my training, experience, and participation in this investigation to date, including my conversations with other FBI agents who have themselves spoken with employees of the Securities and Exchange Commission (the “SEC”) and my own conversations with SEC employees, I have learned the following:

a. On or about December 12, 2022, a Grand Jury in the Southern District of New York returned a sealed Indictment charging Lawrence Billimek and Alan Williams with insider trading

securities fraud, wire fraud, and conspiracy to commit both. The Indictment is attached hereto as Exhibit A and incorporated as if set forth fully herein.

b. A particular type of insider trading is known as “front running.” Generally, front-running schemes involve insider trading based on information an individual learns about a future transaction that will impact the price of an asset—for example, a future large transaction by another trader that will cause an asset’s price to rise or fall. Based on this advance knowledge, the individual can place timely, profitable securities trades in advance of the anticipated large transaction and profit when price of the security rises or falls.

c. In this case, Alan Williams, the Subject Person and a resident of the Subject Premises, appears to be front running trades conducted by the Teachers Insurance and Annuity Association of America College Retirement Equities Fund (“TIAA-CREF”) Investment Management (“TCIM”). I believe Lawrence Billimek to be an equity trader at TCIM, who I believe to be subject to TCIM’s code of ethics prohibiting trading on knowledge of TCIM’s anticipated transactions. (*See* Ind. ¶ 5).<sup>1</sup> To date, the investigation has revealed that Williams and

---

<sup>1</sup> Based on my review of a copy of a form ADV publicly filed by TCIM on or about March 31, 2022, I have learned that TCIM employs Nuveen’s Code of Ethics and TCIM’s Supplemental Code of Ethics (collectively, the “Code”) under Rule 204A-1 of the Investment Advisers Act and Rule 17j-1 of the Investment Company Act. In part, the Code governs the personal trading activities of certain employees or “Access Persons” and members of their households. Based on my review of the TCIM form ADV, I have learned that, among other things, it outlines that Access Persons “[m]ay not attempt to profit personally from their knowledge of recent or contemplated transactions in clients’ accounts including any mutual funds affiliated with” TCIM. In addition, it requires Access Persons to “act in a manner consistent with that of a fiduciary with respect to client accounts” and to “avoid any actual or potential conflict of interest or any abuse of a position of trust and responsibility.” It also prohibits Access Persons from purchasing or selling “a security when they have actual knowledge that a mutual fund or other client account will be trading in that security (or a related security).” Finally, based on my review of a previously published, publicly available version of the Nuveen Code of Ethics and TCIM code of ethics, I have learned that they have defined Access Persons to include, among others, any employee who has access to non-public information regarding the purchase or sale of securities by any fund or client account. Based on my training and experience, and based on Billimek’s job title and description as contained in

Billimek have had communications over the phone and have exchanged electronic messages and have also exchanged emails, including relating to trading activity and on days with suspicious trading. In addition, Williams has paid Billimek at least millions of dollars during the course of the scheme. (*See* Ind. ¶¶ 1-4, 7).

d. To date, the SEC has identified over a thousand examples of apparent front-running trading by Williams in advance of TCIM trades that impacted relevant share prices, which the SEC has determined appears to be ongoing.<sup>2</sup> (*See* Ind. ¶ 8). More specifically, during certain days of this pattern of trading, Williams conducted multiple intra-day trades on single stock tickers, that corresponded to trades that same day by TCIM. (*See* Ind. ¶ 7). To date, the SEC's ongoing trading analysis has revealed that Williams has had hundreds of days of multi-trade intra-day trading and appears to have made at least approximately tens of millions of dollars from this trading, at least some of which corresponds to TCIM trading in the same securities. Certain examples of this trading pattern are outlined in the Indictment at Paragraph 7(d).

e. In general, the profitability of Williams's trading increased significantly in or about September 2016, when his trading appears to begin to align with TCIM's trading in the same stocks. Between in or about September 2016 and August 2022, the profitability of Williams's trading on trades aligned to TCIM trades appears to have significantly surpassed the profitability of his trading on trades that do not align to TCIM trading. In fact, based on the investigation to

---

publicly available information, I believe that the TCIM code of ethics applies to Billimek, and I further believe he would have access to such non-public information as part of his employment and thus qualify as an "access person" subject to the Code.

<sup>2</sup> A review of this trading is ongoing, and the Government has not yet obtained precise times for most of the trades in question by TCIM. In addition, given the ongoing, covert nature of this investigation, the Government may not have received all records of TCIM's trading in these stocks and others, and this Affidavit reflects the records received by the Government to date.

date, it appears that almost all of Williams's trading profits during this time period came from trades that were aligned in timing to TCIM trades in the same stocks. (*See* Ind. ¶ 8).

7. In addition, based on my review of material received from financial institutions, I have learned, in part, that Williams has written checks made out to Billimek totaling, at least, approximately millions of dollars, during this time frame. For example:

- on or about December 18, 2018, Williams wrote a check for \$50,000 to Billimek;
- on or about January 9, 2019, Williams wrote a check for \$50,000 to Billimek;
- on or about January 28, 2019, Williams wrote a check for \$50,000 to Billimek;
- on or about December 22, 2020, Williams wrote a check for \$70,000 to Billimek;
- on or about March 30, 2021, Williams wrote a check for \$80,000 to Billimek;
- on or about July 29, 2021, Williams wrote a check for \$85,000 to Billimek;
- on or about October 20, 2021, Williams wrote a check for \$90,000 to Billimek;
- on or about November 20, 2021, Williams wrote a check for \$374,000 to Billimek;
- on or about December 4, 2021, Williams wrote a check for \$262,000 to Billimek;
- on or about December 13, 2021, Williams wrote a check for \$337,000 to Billimek;
- on or about December 27, 2021, Williams wrote a check for \$240,000 to Billimek.

Some of these checks were written within days of when Williams engaged in profitable intra-day trades that closely aligned with trades in the same stock by TCIM. (*See* Ind. ¶ 9).

8. Based on the foregoing and further information below, there is probable cause to believe that Lawrence Billimek had access to material non-public information about anticipated TCIM trading and Billimek provided this information to Williams, who then traded on the information and paid Billimek a portion of the millions of dollars he profited.



**B. Probable Cause Justifying Search of the Subject Premises**

9. For the reasons set forth below, there is probable cause to believe that the Subject Premises and the electronic devices in the possession of the Subject Person will contain evidence, fruits, and instrumentalities of the Subject Offenses, and that there will be other evidence of the Subject Offenses at the Subject Premises.

Use of Electronic Devices During the Subject Offenses

10. Based on my training, experience, and participation in this investigation to date, including my conversations with other FBI agents who have themselves spoken with employees of the SEC, I have learned the following:

Cellphones Used by Billimek and Williams

a. Lawrence Billimek has been linked to at least three cell phones relevant to this investigation. The first is a cellphone assigned call number 808-666-1150 (the “1150 Phone”). The subscriber name for the 1150 Phone is Lawrence Billimek.<sup>3</sup> The second is a cellphone assigned call number 913-329-2725 (the “2725 Phone”). As further detailed below, I believe that Billimek is the user of the 2725 Phone, which is a prepaid phone.<sup>4</sup> The third is a cellphone assigned call number 310-927-5666 (the “5666 Phone” and, collectively with the 2725 Phone, the “Burner

---

<sup>3</sup> In addition to the subscriber name, I believe that Billimek uses the 1150 Phone based on my review of financial and other records in which he has listed it as his phone number; and my review of GPS data which has placed the 1150 Phone in the vicinity of properties owned by Billimek.

<sup>4</sup> I believe that Billimek uses the 2725 Phone based on, among other things, that the 2725 was purchased in Hawaii, where Billimek owns property; that the 2725 Phone has been in frequent contact with Williams; that use of the 2725 Phone began when use of the 5666 Phone, defined below, slowed or stopped, and thus it appears the 2725 Phone replaced the 5666 Phone; and GPS information has revealed that the 2725 Phone and the 1150 Phone have been frequently co-located in locations associated with Billimek, including the Subject Premises.



Phones”)<sup>5</sup>. As further detailed below, I believe that Billimek formerly used the 5666 Phone, which is also a prepaid phone.

b. Alan Williams has been linked to at least one cell phone relevant to this investigation. The cellphone is assigned call number 510-912-4186 (the “4186 Phone”). The subscriber name for the 4186 Phone is Alan Williams.<sup>6</sup>

Cellphone Use by Billimek and Williams During Pattern of Insider Trading

c. On four occasions, including on or about December 9, 2022 (the “GPS Warrants”), a Magistrate Judge in the Southern District of New York has authorized the Government to receive prospective location information, historical location information, toll records, and pen register information, for the 1150 Phone, 2725 Phone, 4186 Phone, and/or 0618 Phone. Based on my review of material received in connection with the GPS Warrants, and conversations with other FBI agents on the same, I have learned that Billimek and Williams have engaged in significant communication, including on days of suspicious trading and at times aligning with certain of that trading. For example, more specifically:

i. On or about June 8, 2020, Williams, using the 4186 Phone, exchanged approximately 50 text messages with Billimek, using the 5666 Phone. (*See* Ind. ¶ 7(d)(i)).

---

<sup>5</sup> I believe that Billimek used the 5666 Phone based on, among other things, that it was registered on or about August 30, 2016, right around the approximate time that the conspiracy began; and that Billimek, using a Google account registered in his name and lawfully searched pursuant to a Search Warrant issued by a Magistrate Judge in the Southern District of New York, searched for the zip code for Lenexa Kansas on multiple occasions, including right after searching for “Boost Mobile,” and the zip code for the 5666 Phone is the zip code for Lenexa Kansas. In addition, as detailed above, use of the 5666 Phone stopped around the time that the 2725 Phone began, and the 2725 Phone has since been often co-located with Billimek’s personal phone, the 1150 Phone.

<sup>6</sup> In addition to the subscriber name, I believe that Williams uses the 4186 Phone based on my review of financial and other records in which he has listed it as his phone number; and my review of GPS location information that has placed the 4186 Phone at a location I know to be his home.

ii. On or about July 10, 2020, Williams, using the 4186 Phone, exchanged approximately 58 text messages with Billimek, using the 5666 Phone. (*See* Ind. ¶ 7(d)(ii)).

iii. In addition, on or about February 24, 2022, Williams, using the 4186 Phone, texted Billimek, using the 1150 Phone, “must be problems with txt on other #,” which appears to be a reference to the burner phone (which would then have been the 5666 Phone). Billimek wrote to Williams “Sell at 9,” and Williams responded “Flat?” Billimek then wrote “Yes flat[.] We got out ok[.]” Williams engaged in two trades on February 24 “front running” TIAA-CREF trading in the same securities that day. Regarding one of those securities, Vipshop Holdings Ltd., Williams sold approximately 218,000 shares between 10:24 am and 11:27 am, for proceeds of approximately \$1.95 million. This corresponds to an average share sale price of approximately 8.94 dollars—just under the “9” texted by Billimek to Williams.<sup>7</sup> (*See* Ind. ¶ 7(d)(iii)).

#### Ongoing Phone Connectivity

d. Based on my review of material received in connection with the GPS Warrants, and conversations with other FBI agents on the same, I have learned that Billimek and Williams remain in frequent communication. More specifically:

i. Between on or about November 4 and December 4, 2022, Williams, using the 4186 Phone, exchanged approximately 44 text messages with Billimek, using the 1150 Phone.

///

///

///

---

<sup>7</sup> The content of these messages was obtained pursuant to a judicially-authorized search warrant of an iCloud account associated with Billimek (which is, among other things, registered in his name), to which he had “backed up” certain of his messages.

ii. Between on or about November 4 and December 4, 2022, Williams, using the 4186 Phone, exchanged approximately 432 text messages with Billimek, using the 2725 Phone.<sup>8</sup>

11. In summation, in addition to the suspicious trading outlined above, the investigation has also revealed that Alan Williams has paid Lawrence Billimek at least approximately \$10 millions dollars; and that Williams and Billimek have remained in communication during days of significant trading by Williams front-running TIAA trades, including through the use of prepaid burner phones.

Alan Williams and the Subject Premises

12. The applied-for warrants would authorize the search of (a) Alan Williams's person and (b) the Subject Premises as well as any closed containers or items contained therein, and the seizure and forensic examination of any electronic device belonging to Alan Williams seized from him or the Subject Premises for the purpose of identifying electronically stored data or other evidence, fruits, or instrumentalities of the Subject Offenses, as particularly described in Attachments A-1, A-2, B-1, and B-2, and for certain other financial and trading records (as well as materials evidencing the relationship between Billimek and Williams) that may be found at the Subject Premises, as also particularly described in Attachment A. As described below, there is probable cause to believe that electronic devices are likely to be found on Alan Williams's person or in the Subject Premises, which is one of his homes and the one at which he appears to be presently residing, and that those electronic devices, including one or more cellphones and

---

<sup>8</sup> At certain times in the summer and fall of 2022, there appear to have been no text messages sent by the 2725 Phone. However, the 2725 Phone remained powered on for at least some of this time, and it remained co-located with the 1150 Phone, including to locations where I know Billimek owns property.

computers, were used as instrumentalities of and contain evidence of the Subject Offenses, as further described below, and contain evidence of the same, and that other materials, including financial and trading recordings, will be located at the Subject Premises, and contain evidence of the Subject Offenses.

13. First, there is probable cause to believe that Alan Williams is in possession of electronic devices, and that those devices are likely to be found on his person or in the Subject Premises, which is where he currently resides:

a. Based on my review of records obtained from financial institutions, including JP Morgan Chase Bank, I know that Williams has listed the Subject Premises as his address in connection with certain of his bank accounts. Based on my training and experience, I know that individuals often list the place where they live as a mailing address for financial institutions where they have accounts.

b. Based on cellphone location information provided pursuant to the GPS Warrants, I have learned that the 4186 Phone is currently located in the District of Oregon and is often in the vicinity of the Subject Premises, including late at night or in early morning hours when Williams would likely be sleeping.

c. Based on my training and experience, I know that individuals who are involved in conduct like the Subject Offenses will often use their computers—at home and/or at work—to, among other things, communicate with co-conspirators; execute trades; follow the financial markets; and research stocks they have confidential inside information about.

d. I know from my training and experience that when individuals are not home, they often take their cellphone(s) with them, and therefore if the 4186 Phone is not in the Subject Premises, it is likely to be on Williams's person. Indeed, based on my review of the cellphone

location information for the phones, it appears that they sometimes move from the vicinity of the Subject Premises, which appears to indicate that Williams is taking his cellphone with him when he leaves the Subject Premises.

e. Accordingly, there is probable cause to believe that Alan Williams lives at the Subject Premises and that his electronic devices will be found on his person or in the Subject Premises.

14. Second, there is probable cause to believe Alan Williams's electronic devices will contain evidence and instrumentalities of the commission of the Subject Offenses. In particular:

a. As set forth above, there is probable cause to believe that Alan Williams used the 4186 Phone to communicate with co-conspirator(s) in the commission of the Subject Offenses. Specifically, Williams communicated by cellphone with, among others, Lawrence Billimek, who provided Williams with confidential information on which Williams then traded. As described above, Billimek and Williams appear to have used two pre-paid "burner" phones to communicate and also the cellular phone registered to Billimek. Regarding the former, based on my training and experience, I know individuals often use pre-paid "burner" phones during the commission of crimes like insider trading in an effort to evade law enforcement scrutiny and hide their activity if they are under investigation. Regarding the latter, certain of the communications already obtained by the Government evidence that Billimek instructed Williams when and at what price to trade. Accordingly, and based on the communication records summarized above, as well as my training and experience, there is probable cause to believe that Williams's cell phone(s) will contain evidence of those communications, as well as other evidence of the commission of the Subject Offenses, including call logs, voicemail messages, text messages, email correspondence, email attachments and loose documents, contact information of co-conspirators and/or witnesses, notes

about calls and meetings, internet search history relating to unlawful conduct (such as, for instance, searching the price of certain securities), images and videos (including screenshots and/or recordings of communications), and logs of communication with co-conspirators and/or witnesses over messaging applications.

b. In addition, based on my training and experience, I know that Alan Williams's electronic devices are likely to contain location information that may be evidence that certain subjects of the investigation were located in the same place at a relevant period in time. Such location information may include cellphone location data, IP records, photographs of locations, and/or calendar entries, and may establish that, for instance, two members of the conspiracy were together at, around, or shortly before the time one member of the conspiracy traded in stock based on misappropriated confidential information.

c. Further, based on my training and experience, I know that Alan William's electronic devices may contain evidence of his knowledge of the prohibition against insider trading in securities. Such evidence may include emails, texts, or documents discussing insider trading; or web history or search history relating to insider trading or Williams's state of mind. Such records may also contain evidence of consciousness of guilt following trading by Williams.

d. In addition, based on my training and experience, I have learned that individuals engaged in criminal activity often store such records, sometimes for years, as records of past relationships with co-conspirators, to keep track of co-conspirator's contact information, to keep a record of transactions, to store passwords or account information or accounts or devices used in furtherance of the criminal activity, or notes to follow up on other aspects of the scheme.

15. Third, I know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to

establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to commit the crimes described in this affidavit. I also know from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched.

16. Lastly, in addition to electronic devices, I respectfully submit that there is probable cause to believe that the Subject Premises may contain additional evidence of the Subject Offenses. I know from training and experience that individuals involved in offenses like the Subject Offenses often maintain bank and trading records related to the crimes; including, for example, records received from financial institutions that evidence payment and trading history or notes of calls and discussions with co-conspirators. Indeed, during this investigation, the Government has obtained banking and trading records related to Billimek and Williams; copies of the same or similar records may be located at the Subject Premises. So, too, may the Subject Premises contain ledgers evidencing trading by Williams or payments from Williams to Billimek, which I know, based on my training and experience, individuals involved in offenses like the Subject Offenses often maintain. In addition, the Subject Premises may contain additional evidence of the relationship between the co-conspirators; such as, for example, photographs of Billimek and Williams together.

**C. Search of ESI for Evidence of the Subject Offenses**

17. Based on the foregoing, there is probable cause to believe that any electronic devices in the possession of Alan Williams or on the premises of the Subject Premises (collectively, the “Subject Devices”), contain evidence, fruits, and instrumentalities of the Subject Offenses. In particular, I believe the Subject Devices are likely to contain the following information:

///



a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses consisting of registration information, access logs, device information, user photographs, contact information, payment information, and other personally identifiable information.

b. Communications between Lawrence Billimek and Alan Williams related to securities trading and/or evidencing the relationship among them.

c. Evidence of knowledge of the prohibition against insider trading in securities.

d. Evidence of Lawrence Billimek's access to material non-public information, including trade orders from TCIM.

e. Evidence of Lawrence Billimek's or Alan Williams's ownership and control over brokerage accounts, and history of trading securities.

f. Evidence of trading by Williams on the basis of information provided by Billimek, including, but not limited to, information provided by Billimek to Williams and updates from Williams to Billimek about ongoing purchases and sales.

g. Evidence of the existence of relationships between Lawrence Billimek and Alan Williams.

h. Evidence of the receipt, transfer, disposition or location of funds raised through the commission of the Subject Offenses.

i. Evidence of efforts to conceal the commission of the Subject Offenses and evade detection by law enforcement and/or regulatory agencies.

j. Evidence of the geographic location of the user(s) of the Subject Devices, as well as other electronic devices used, including records of or information about Internet Protocol addresses used in connection with the Subject Devices.

k. Evidence of passwords or other information needed to access the Subject Devices.

l. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

18. Based on my training and experience, I also know that, where electronic devices are used in furtherance of criminal activity, such as the Subject Devices, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

a. Electronic files can be stored on an electronic drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

b. Things that have been viewed via the Internet are typically stored for some period of time on digital devices.

c. Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on an electronic device, the data contained in the file does not actually disappear, but instead remains, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the device. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from an electronic device depends less on when the file was created or viewed than on a particular user’s operating system, storage capacity, and user habits.

d. In the event that a user changes electronic devices, the user will typically transfer files from the old device to the new device, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

19. In addition to there being probable cause to believe that the Subject Devices contain evidence of the Subject Offenses, there is also probable cause to believe that the Subject Devices constitute instrumentalities of the Subject Offenses, because they were used to communicate with co-conspirators in furtherance of the Subject Offenses.

### **III. Procedures for Searching ESI**

#### **A. Unlocking Devices with Biometric Features**

20. I request authority to allow law enforcement agents to obtain from Alan Williams (but not any other individuals present at the Subject Premises at the time of execution of the warrants) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the physical biometric characteristics of Alan Williams will unlock the device(s). This authority is not to compel Alan Williams to provide a numeric passcode. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed above, there is reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to

know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

21. Due to the foregoing, I respectfully request that the Court authorize that, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, law enforcement personnel may obtain from Alan Williams the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of Alan Williams to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Alan Williams to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Alan Williams to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by the proposed warrants.

#### **B. Execution of Warrant for ESI**

22. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

a. First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized

software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

c. Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

### **C. Review of ESI**

23. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

24. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

a. surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);



- b. conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- c. “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- d. performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation;<sup>9</sup> and
- e. reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

25. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

26. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of

---

<sup>9</sup> Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

27. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

28. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

29. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

30. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

#### **IV. Conclusion**

31. Based on the foregoing, I respectfully request the court to issue warrants to seize the items and information specified in Attachments B-1 and B-2 to this affidavit and to the search and seizure warrants.

32. Prior to being submitted to the Court, this affidavit, the accompanying applications, and the requested search warrants were all reviewed by Assistant United States Attorney Seth D. Uram and AUSA Uram advised me that in his opinion the affidavit and applications are legally and factually sufficient to establish probable cause to support the issuance of the requested warrants.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

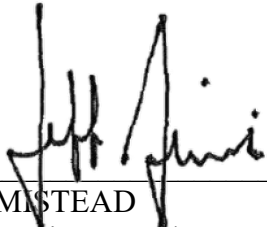
///

**V. Request for Sealing**

33. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrants and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

By telephone pursuant to Fed.R.Crim. 4.1  
Flynn McFadden  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn in accordance with the requirements of Fed.R.Crim.P. 4.1 by telephone at  
4:15 pm on December 13, 2022.

  
\_\_\_\_\_  
JEFFREY ARMISTEAD  
United States Magistrate Judge



the confidential trade information from BILLIMEK, thereby earning tens of millions of dollars in illicit profit.

2. In return for the confidential trade information, ALAN WILLIAMS, the defendant, sent at least approximately ten million dollars back to LAWRENCE BILLIMEK, the defendant, as payment for the confidential trade information. In describing the nature and source of these payments, WILLIAMS and BILLIMEK provided false and misleading information to various financial institutions, including that the payments were gifts to BILLIMEK. WILLIAMS and BILLIMEK remained in close and regular contact throughout the scheme to share the confidential trade information, including through the use of pre-paid unsubscribed "burner" phones.

#### Relevant Individuals and Entities

3. LAWRENCE BILLIMEK, the defendant, is a trader at the Employer, where he has worked since in or about 2012. BILLIMEK has previously worked as a trader at other financial firms. Prior to engaging in this illegal front running scheme, BILLIMEK had substantial financial troubles. For example, in an email in or about August 2016, BILLIMEK wrote that he was "struggling" financially and "living paycheck to paycheck."

4. The Employer is an SEC registered investment advisor headquartered in New York, New York, which provides advisory services to a large investment management company that manages over \$200 billion in assets.

5. At all relevant times, the Employer has maintained a code of ethics (the "Code of Ethics") that governs the personal trading activities of certain employees, including equity traders like LAWRENCE BILLIMEK, the defendant. The Code of Ethics regulates the use of confidential information that employees like BILLIMEK receive in the course of their employment, and prohibits, among other things, any effort to profit personally from their knowledge of recent or contemplated transactions in any account managed by the Employer. Among other things, the Code of Ethics also incorporated other prohibitions, including a strict prohibition on "front-running or tailgating (trading directly before or after the execution of a large client trade order), or any attempt to influence a client's trading to enhance the value of your personal holdings."

6. ALAN WILLIAMS, the defendant, is the former head equity trader at a large investment firm. WILLIAMS holds multiple retail trading accounts and actively day trades in at least two retail trading accounts.

#### Means and Method of the Scheme

7. From at least in or about 2016 through in or about the present, LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, engaged in a front-running scheme to earn millions of dollars based on timely, profitable trading based on stolen inside information obtained from BILLIMEK in violation of BILLIMEK's duties of trust



and confidentiality to the Employer. In particular, the illegal scheme has had three basic elements:

a. First, BILLIMEK obtains confidential information about upcoming trades that the Employer intends to execute in certain securities (the "Confidential Trade Information"). Given the large sizes of these trades, they are likely to and often do cause a temporary move in the price of the underlying security. For example, a large buy order by the Employer would be likely to cause a temporary increase in the price of the underlying security due to the demand pressure generated by that buy order.

b. Second, BILLIMEK then shares the Confidential Trade Information with WILLIAMS. Over the course of the scheme, BILLIMEK typically has shared that information with WILLIAMS through phone calls or text messages, including through the use of at least two pre-paid unregistered "burner" phones used by BILLIMEK.

c. Third, WILLIAMS then uses the Confidential Trade Information to place timely, profitable securities trades. These trades are typically short-term intraday trades designed to take advantage of the temporary price movements caused by the underlying stock trading that is the subject of the Confidential Trade Information.

d. The following are certain examples of the trading scheme:

i. On or about June 8, 2020, WILLIAMS, based on Confidential Trade Information, realized profits of approximately \$121,000 on intraday trading in shares of Lululemon Athletica Inc. ("LULU"). In particular, WILLIAMS engaged in a short sale of LULU shares just before the Employer engaged in the sale of a substantial number of LULU shares, and then WILLIAMS covered his short position at a lower price following the Employer's transactions.

ii. On or about July 10, 2020, WILLIAMS, based on Confidential Trade Information, realized profits of approximately \$179,000 on intraday trading in shares of Ulta Beauty, Inc. ("ULTA"). In particular, WILLIAMS engaged in short sale of ULTA shares just before the Employer engaged in the sale of a substantial number of ULTA shares, and then WILLIAMS covered his short position at a lower price following the Employer's transactions.

iii. On or about February 24, 2022, WILLIAMS, based on Confidential Trade Information, realized profits of approximately \$55,000 on intraday trading in shares of Vipshop Holdings Ltd ("VIPS"). In particular, between approximately 9:51 and 10:15 a.m. that morning, WILLIAMS bought over \$1.8 million of VIPS shares, shortly before the Employer engaged in the purchase of a substantial number of VIPS shares. Then, within minutes, between

approximately 10:24 and 10:26 a.m., WILLIAMS sold all of the VIPS shares at a higher price following the Employer's transactions.

iv. On or about August 15, 2022, WILLIAMS, based on Confidential Trade Information, realized profits of approximately \$55,500 in intraday trading in shares of Match Group Inc. ("MTCH"). In particular, WILLIAMS sold short shares of MTCH just before the Employer engaged in the sale of a substantial number of MTCH shares, and then WILLIAMS covered his short position at a lower price following the Employer's transactions.

8. Over the course of the scheme, ALAN WILLIAMS, the defendant, has engaged in over approximately a thousand intraday trades based on Confidential Trade Information provided by LAWRENCE BILLIMEK, the defendant. This trading has been spectacularly profitable, particularly when compared to other securities trading that WILLIAMS has conducted. In particular, since in or about September 2016, WILLIAMS' intraday trading has consistently been profitable over 90 percent of the time, leading to profits of tens of millions of dollars. By contrast, WILLIAMS' non-intraday securities trading during the relevant period has, overall, resulted in a net loss.

9. As part of their scheme, LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, agreed to share and have shared their illicit proceeds, including through the use of checks and wire transfers from WILLIAMS to BILLIMEK. In order to conceal the

nature and source of these payments, BILLIMEK and WILLIAMS have lied about the true nature of the payments, including by calling them gifts. At times, BILLIMEK has also authored affidavits or letters for WILLIAMS to sign and submit to his financial institutions to obfuscate the true source of these funds, and has claimed at various times, a family relationship or close friendship to explain the reason for the transfer of funds. In total, WILLIAMS has transferred millions of dollars back to BILLIMEK in return for the lucrative Confidential Trade Information.

#### Statutory Allegations

10. From at least in or about 2016 through in or about the present, in the Southern District of New York and elsewhere, LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, and wire fraud, in violation of Title 18, United States Code, Section 1343.

11. It was a part and object of the conspiracy that LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, and others known and unknown, willfully and knowingly, directly and indirectly, by the use of a means and instrumentality of interstate commerce and of



the mails, and of a facility of a national securities exchange, would and did use and employ, in connection with the purchase and sale of a security registered on a national securities exchange and a security not so registered, and a securities-based swap agreement, a manipulative and deceptive device and contrivance, in violation of Title 17, Code of Federal Regulation, Section 240.10b-5, by: (a) employing a device, scheme, and artifice to defraud; (b) making an untrue statement of material fact and omitting to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (c) engaging in an act, practice, and course of business which operated and would operate as a fraud and deceit upon a person, in violation of Title 15, United States Code, Section 78j(b) and 78ff.

12. It was further a part and an object of the conspiracy that LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such

scheme and artifice, in violation of Title 18, United States Code, Section 1343.

Overt Acts

13. In furtherance of the conspiracy and to effect its illegal objects, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about June 8, 2020, LAWRENCE BILLIMEK, the defendant, shared Confidential Trade Information with ALAN WILLIAMS, the defendant, after which WILLIAMS engaged in timely, profitable trading in the shares of LULU.

b. On or about July 10, 2020, BILLIMEK shared Confidential Trade Information with WILLIAMS, after which WILLIAMS engaged in timely, profitable trading in the shares of ULTA.

(Title 18, United States Code, Section 371.)

COUNT TWO  
(Securities Fraud)

The Grand Jury further charges:

14. The allegations contained in paragraphs 1 through 9 of this Indictment are hereby repeated, realleged, and incorporated by reference, as if fully set forth herein.

15. From at least in or about 2016 through in or about the present, in the Southern District of New York and elsewhere, LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, willfully and knowingly, directly and indirectly, by the use of a means and

instrumentality of interstate commerce and of the mails, and of a facility of a national securities exchange, used and employed, in connection with the purchase and sale of a security registered on a national securities exchange and a security not so registered, and a securities-based swap agreement, a manipulative and deceptive device and contrivance, in violation of Title 17, Code of Federal Regulation, Section 240.10b-5, by: (a) employing a device, scheme, and artifice to defraud; (b) making an untrue statement of material fact and omitting to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (c) engaging in an act, practice, and course of business which operated and would operate as a fraud and deceit upon a person, to wit, BILLIMEK fraudulently misappropriated confidential information from the Employer about the Employer's confidential securities trade orders and trading activity, and shared that information with WILLIAMS to enable WILLIAMS to place timely, profitable securities trades based on that information.

(Title 15, United States Code, Sections 78j(b) & 78ff;  
Title 17, Code of Federal Regulations, Sections 240.10b-5,  
240.10b5-1, and 240.10b5-2; and Title 18, United States Code,  
Section 2.)

COUNT THREE  
(Wire Fraud)

The Grand Jury further charges:

16. The allegations contained in paragraphs 1 through 9 of this Indictment are hereby repeated, realleged, and incorporated by reference, as if fully set forth herein.

17. From at least in or about 2016 through in or about the present, in the Southern District of New York and elsewhere, LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, BILLIMEK misappropriated confidential information from the Employer about the Employer's confidential securities trade orders and trading activity, and shared that information with WILLIAMS to enable WILLIAMS to place timely, profitable securities trades based on that information, which scheme involved the use of interstate wires.

(Title 18, United States Code, Sections 1343 and 2.)



FORFEITURE ALLEGATION

18. As a result of committing the offenses charged in Counts One through Three of this Indictment, LAWRENCE BILLIMEK and ALAN WILLIAMS, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses and the following specific property:

a. Any and all funds and assets up to and including \$6,476,123 of U.S. currency and securities held in TD Ameritrade brokerage account number 780-078556 in the name of Alan Williams, and all proceeds traceable thereto;

b. Any and all funds and assets up to and including \$7,806,920 of U.S. currency and securities held in TD Ameritrade brokerage account number 875-327835 in the name of the Alan G. Williams Trust, and all proceeds traceable thereto;

c. Any and all funds up to and including \$17,932,268 of U.S. currency in JP Morgan Chase account number 3132113303 held in the name of Alan Williams, and all proceeds traceable thereto;

d. Any and all funds up to and including \$461,000 of U.S. currency in JP Morgan Chase account number 1854194099 held in the name of Alan Williams, and all proceeds traceable thereto;

e. Any and all funds up to and including \$3,695,000 of U.S. currency in JP Morgan Chase account number 444961200 held in the name of the Alan G. Williams Income Trust, and all proceeds traceable thereto;

f. The real property located at 1095 SW Schaeffer Road, West Linn, Oregon, and all proceeds traceable thereto;

g. Any and all funds up to and including \$4,196,000 of U.S. currency in JP Morgan Chase account number 3606375211 held in the name of Lawrence P. Billimek, and all proceeds traceable thereto;

h. \$150,000 of value in the Scenic Capital Advisors HIES Medical Center, LLC, and all proceeds traceable thereto;

i. The real property located at 25 South Club View Drive, Hailey, Idaho, and all proceeds traceable thereto;

j. The real property located at 1220 Dauphine Street, Unit F, New Orleans, Louisiana, and all proceeds traceable thereto;

k. The real property located at 56854 Besson Road, Bend, Oregon, and all proceeds traceable thereto;

l. The real property located at 5808 Beacon Drive, Austin, Texas, and all proceeds traceable thereto;

m. The real property located at 1903 Eva Street, Austin, Texas, and all proceeds traceable thereto;

n. The real property located at 4460 Aku Road, Hanalei, Hawaii, and all proceeds traceable thereto;

o. The real property located at 181 Hyndman View Drive, Hailey, Idaho, and all proceeds traceable thereto; and

p. The real property located at 147 Magnolia Drive, San Antonio, Texas, and all proceeds traceable thereto.

Substitute Assets Provision

19. If any of the above-described forfeitable property, as a result of any act or omission by the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), and Title 28, United States Code Section 2461, to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described above.

(Title 18, United States Code, Sections 981(a)(1)(C);  
Title 21, United States Code, Section 853(p);  
Title 28, United States Code, Section 2461.)



FOREPERSON



DAMIAN WILLIAMS  
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

---

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

---

UNITED STATES OF AMERICA

- v. -

LAWRENCE BILLIMEK and  
ALAN WILLIAMS,

Defendants.

---

SEALED INDICTMENT

22 Cr. \_\_\_\_\_

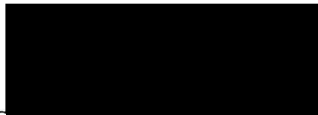
(Title 15, United States Code, Sections  
78j(b) and 78ff; Title 17, Code of Federal  
Regulations, Sections 240.10b-5, 240.10b5-  
1, 240.10b5-2; Title 18, United States  
Code, Sections 2, 371, and 1343.)

---

DAMIAN WILLIAMS  
United States Attorney

---

A TRUE BILL



---

Foreperson

---

**ATTACHMENT A-1**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

1095 SW Schaeffer Road, West Linn, OR 97068. Publicly available photographs of the Subject Premises are depicted below:





**ATTACHMENT B-1**

**ITEMS TO BE SEIZED FROM THE PREMISES**

The items to be searched for, seized, and examined are those items located at the Premises identified in Attachment A-1, that contain or are evidence, fruits, and instrumentalities of violations of 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b-5 (insider trading securities fraud); 18 U.S.C. § 1343 (wire fraud); and aiding and abetting and conspiring to commit these offenses in violation of 18 U.S.C. §§ 2 (aiding and abetting), 371 (conspiracy), and 1349 (conspiracy).

1. Law enforcement agents are authorized to seize any and all cellphones, tablets, computers, and electronic storage media within the Subject Premises (collectively, the “Subject Devices”). In lieu of seizing any Subject Device, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

(a) Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

(b) Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

(c) Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

During the execution of the warrant, law enforcement personnel are authorized to obtain from Alan Williams the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Subject Devices, including to (1) press or swipe the fingers (including thumbs) of Alan Williams to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Alan Williams to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Alan Williams to

activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

2. Following seizure of any Subject Devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant, and described as follows:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses consisting of registration information, access logs, device information, user photographs, contact information, payment information, and other personally identifiable information.

b. Communications between Lawrence Billimek and Alan Williams related to securities trading and/or evidencing the relationship among them.

c. Evidence of knowledge of the prohibition against insider trading in securities.

d. Evidence of Lawrence Billimek's access to material non-public information, including trade orders from TCIM.

e. Evidence of Lawrence Billimek's or Alan Williams's ownership and control over brokerage accounts, and history of trading securities.

f. Evidence of trading by Williams on the basis of information provided by Billimek, including, but not limited to, information provided by Billimek to Williams and updates from Williams to Billimek about ongoing purchases and sales.

g. Evidence of the existence of relationships between Lawrence Billimek and Alan Williams.

h. Evidence of the receipt, transfer, disposition or location of funds raised through the commission of the Subject Offenses.

i. Evidence of efforts to conceal the commission of the Subject Offenses and evade detection by law enforcement and/or regulatory agencies.



j. Evidence of the geographic location of the user(s) of the Subject Devices, as well as other electronic devices used, including records of or information about Internet Protocol addresses used in connection with the Subject Devices.

k. Evidence of passwords or other information needed to access the Subject Devices.

l. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

3. In addition to cellphones, tablets, computers, and electronic storage media within the Subject Premises, law enforcement personnel are authorized to search the Subject Premises for additional materials responsive to the warrant, described as follows:

a. Financial records, including but not limited to bank and trading records.

b. Ledgers and notes concerning trading by or communications between Lawrence Billimek and Alan Williams.

c. Evidence of payments among and between Lawrence Billimek and Alan Williams.

d. Evidence of the relationship between Lawrence Billimek and Alan Williams including but not limited to photographs.

4. In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

5. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Devices to their owner within a reasonable period of time following the search and will seal any image of the Devices, absent further authorization from the Court.

8. If the Devices contain evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Devices and/or the data contained therein.

9. The government will retain a forensic image of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

**ATTACHMENT A-2**

The person to be searched is Alan Williams, who was born on September 3, 1945, and is depicted in the photograph below:



**ATTACHMENT B-2**

**ITEMS TO BE SEIZED FROM THE PERSON, VICINITY AND CONTROL  
OF ALAN WILLIAMS**

The items to be searched for, seized, and examined are those items located on the person, and within the vicinity and control of Alan Williams, identified in Attachment A-2, that contain or are evidence, fruits, and instrumentalities of violations of 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b-5 (insider trading securities fraud); 18 U.S.C. § 1343 (wire fraud); and aiding and abetting and conspiring to commit these offenses in violation of 18 U.S.C. §§ 2 (aiding and abetting), 371 (conspiracy), and 1349 (conspiracy).

1. This warrant authorizes the search of William's person and his personal effects in the immediate vicinity and control of Williams at the location where the search warrant is executed, including any backpacks, briefcases, purses, and bags. The warrant authorizes the search, seizure, and forensic examination of any and all cellphones, tablets, computers, and electronic storage media within the Subject Premises (collectively, the "Subject Devices"). In lieu of seizing any Subject Device, this warrant also authorizes the copying of such devices or media for later review.

2. During the execution of the warrant, law enforcement personnel are authorized to obtain from Alan Williams the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Subject Devices, including to (1) press or swipe the fingers (including thumbs) of Alan Williams to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Alan Williams to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Alan Williams

to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

3. Following seizure of any Subject Devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant, as follows:

- a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses consisting of registration information, access logs, device information, user photographs, contact information, payment information, and other personally identifiable information.
- b. Communications between Lawrence Billimek and Alan Williams related to securities trading and/or evidencing the relationship among them.
- c. Evidence of knowledge of the prohibition against insider trading in securities.
- d. Evidence of Lawrence Billimek's or Alan Williams's ownership and control over brokerage accounts, and history of trading securities.
- e. Evidence of Lawrence Billimek's access to material non-public information, including TCIM's trade orders.
- f. Evidence of concerning trading by Williams on the basis of information provided by Billimek, including, but not limited to, information provided by Billimek to Williams and updates from Williams to Billimek about ongoing purchases and sales.
- g. Evidence of the existence of relationships between Lawrence Billimek and Alan Williams.
- h. Evidence of the receipt, transfer, disposition or location of funds raised through the commission of the Subject Offenses.
- i. Evidence of efforts to conceal the commission of the Subject Offenses and evade detection by law enforcement and/or regulatory agencies.

j. Evidence of the geographic location of the user(s) of the Subject Devices, as well as other electronic devices used, including records of or information about Internet Protocol addresses used in connection with the Subject Devices.

k. Evidence of passwords or other information needed to access the Subject Devices.

l. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

4. In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

5. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant.

If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Devices to their owner within a reasonable period of time following the search and will seal any image of the Devices, absent further authorization from the Court. If the Devices contain evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Devices and/or the data contained therein.

8. The government will retain a forensic image of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.